

# A Counterexample to the Vector Generalization of Costa's EPI, and Partial Resolution

Thomas A. Courtade\*, Guangyue Han<sup>†</sup> and Yaochen Wu<sup>†</sup>

\*UC Berkeley, Department of Electrical Engineering and Computer Sciences

<sup>†</sup>The University of Hong Kong, Department of Mathematics

April 19, 2017

## Abstract

We give a counterexample to the vector generalization of Costa's entropy power inequality (EPI) due to Liu, Liu, Poor and Shamai. In particular, the claimed inequality can fail if the matrix-valued parameter in the convex combination does not commute with the covariance of the additive Gaussian noise. Conversely, the inequality holds if these two matrices commute.

For a random vector  $X$  with density on  $\mathbb{R}^n$ , we let  $h(X)$  denote its differential entropy. Let  $Z \sim N(0, \Sigma_Z)$  be a Gaussian vector in  $\mathbb{R}^n$  independent of  $X$ , and let  $A$  be a (real symmetric) positive semidefinite  $n \times n$  matrix satisfying  $A \preceq I$  with respect to the positive semidefinite ordering, where  $I$  denotes the identity matrix. In [1, Theorem 1], Liu, Liu, Poor and Shamai claim the following generalization of Costa's EPI<sup>1</sup> [2]:

$$e^{\frac{2}{n}h(X+A^{1/2}Z)} \geq |I - A|^{1/n} e^{\frac{2}{n}h(X)} + |A|^{1/n} e^{\frac{2}{n}h(X+Z)}. \quad (1)$$

Liu et al. apply (1) in their investigation of the secrecy capacity region of the degraded vector Gaussian broadcast channel with layered confidential messages.

The purpose of this note is to demonstrate that (1) can fail for  $n \geq 2$ , and also to offer a partial resolution. Toward the first goal, consider  $n = 2$  and let us define

$$\Sigma_X = \begin{pmatrix} 200 & 100 \\ 100 & 51 \end{pmatrix}, \quad \Sigma_Z = \begin{pmatrix} 200 & 0 \\ 0 & 1 \end{pmatrix}, \quad A^{1/2} = \frac{1}{20} \begin{pmatrix} 10 & 5 \\ 5 & 17 \end{pmatrix}. \quad (2)$$

Taking  $X \sim N(0, \Sigma_X)$  and  $Z \sim N(0, \Sigma_Z)$  to be independent Gaussian vectors, we have

$$\frac{1}{2\pi e} e^{\frac{2}{n}h(X+A^{1/2}Z)} = |\Sigma_X + A^{1/2}\Sigma_Z A^{1/2}|^{1/2} \approx 19.53.$$

On the other hand,

$$\frac{1}{2\pi e} \left( |I - A|^{1/n} e^{\frac{2}{n}h(X)} + |A|^{1/n} e^{\frac{2}{n}h(X+Z)} \right) = |I - A|^{1/2} |\Sigma_X|^{1/2} + |A|^{1/2} |\Sigma_X + \Sigma_Z|^{1/2} \approx 40.28.$$

Thus, a contradiction to (1) is obtained. We remark that there is nothing particularly unique about this counterexample, except that the matrices were chosen to violate (1) by a significant margin.

<sup>1</sup>All entropies are taken to be base  $e$  throughout. Also, for a positive semidefinite matrix  $M$ , we write  $M^{1/2}$  to denote the unique positive semidefinite matrix such  $M = M^{1/2}M^{1/2}$ .

Evidently, further assumptions are needed in order for (1) to hold. As we now argue, it suffices for  $A$  and  $\Sigma_Z$  commute. Fortunately, the critical application of inequality (1) by Liu et al. (see [1, p. 1877]) assumes only that  $A$  and  $\Sigma_Z$  are diagonal matrices, so the main conclusions of [1], aside from [1, Theorem 1], appear to be unaffected. That said, reference [1] has been cited numerous times in the literature, so other published results may be impacted. We do not attempt to give an account of these consequences here, but note that this matter deserves independent attention.

**Theorem 1.** *Let  $X$  be a random vector with density on  $\mathbb{R}^n$ , and let  $Z \sim N(0, \Sigma_Z)$  be a Gaussian vector in  $\mathbb{R}^n$  independent of  $X$ . If  $A \preceq I$  is positive semidefinite and commutes with  $\Sigma_Z$ , then*

$$e^{\frac{2}{n}h(X+A^{1/2}Z)} \geq |I - A|^{1/n} e^{\frac{2}{n}h(X)} + |A|^{1/n} e^{\frac{2}{n}h(X+Z)}.$$

*Proof.* Since both  $A$  and  $\Sigma_Z$  are symmetric, they commute if and only if they are simultaneously diagonalizable; i.e.,  $\Sigma_Z = U\Lambda U^T$  and  $A = UDU^T$ , for  $U$  orthogonal and  $\Lambda, D$  diagonal matrices. Since  $A^{1/2} = UD^{1/2}U^T$  and  $(I - A)^{1/2} = U(I - D)^{1/2}U^T$ , we have the following identity

$$A^{1/2}\Sigma_Z A^{1/2} + (I - A)^{1/2}\Sigma_Z(I - A)^{1/2} = \Sigma_Z. \quad (3)$$

It was established in [3] that if  $X, Y, W$  are independent random vectors in  $\mathbb{R}^n$ , with  $W$  Gaussian, then

$$e^{\frac{2}{n}h(X+W)} e^{\frac{2}{n}h(Y+W)} \geq e^{\frac{2}{n}h(X)} e^{\frac{2}{n}h(Y)} + e^{\frac{2}{n}h(W)} e^{\frac{2}{n}h(X+Y+W)}. \quad (4)$$

To apply this, let  $Y = (I - A)^{1/2}Z_1$  and  $W = A^{1/2}Z_2$ , where  $Z_1, Z_2$  are independent copies of  $Z$ . It follows from (3) that  $Y + W = Z$  in distribution, so that (4) particularizes to

$$e^{\frac{2}{n}h(X+A^{1/2}Z)} e^{\frac{2}{n}h(Z)} \geq |I - A|^{1/n} e^{\frac{2}{n}h(X)} e^{\frac{2}{n}h(Z)} + |A|^{1/n} e^{\frac{2}{n}h(Z)} e^{\frac{2}{n}h(X+Z)}.$$

Dividing through by  $e^{\frac{2}{n}h(Z)}$  completes the proof.  $\square$

**Remark 1.** *The proof above was originally given in [3] as an application demonstrating that (1) could be recovered from (4). However, it was mistakenly claimed that  $(I - A)^{1/2}Z_1 + A^{1/2}Z_2$  was equal in distribution to  $Z$ , which need not hold unless  $A$  and  $\Sigma_Z$  commute.*

It turns out that Liu et al.'s proof is also valid under the assumption that  $A$  and  $\Sigma_Z$  commute. More precisely, Liu et al.'s proof contains an incorrect application of the AM-GM inequality in the form:

$$|\Sigma_Z^{-1} \text{Cov}(Z|D_\gamma X + Z)(I - D_\gamma^{-2})|^{1/n} \leq \frac{1}{n} \text{Tr}(\Sigma_Z^{-1} \text{Cov}(Z|D_\gamma X + Z)(I - D_\gamma^{-2})), \quad (5)$$

where  $D_\gamma := (I + \gamma(A - I))^{1/2}$ , and  $\gamma \in [0, 1]$  parameterizes a path of perturbation. Inequality (5) can fail if the argument of the trace is not positive semidefinite, and a product of positive semidefinite matrices is not necessarily positive semidefinite. For instance, returning to the counterexample above where  $X \sim N(0, \Sigma_X)$  and matrices are chosen according to (2), then the eigenvalues of  $\Sigma_Z^{-1} \text{Cov}(Z|D_\gamma X + Z)(I - D_\gamma^{-2})$  can be computed as being approximately  $\{-0.0053, -0.7273\}$  for  $\gamma = 0.5$ , in violation of (5).

However, if  $A$  and  $\Sigma_Z$  commute, then so do  $\Sigma_Z^{-1/2}$  and  $(I - D_\gamma^{-2})^{1/2}$  (since both are simultaneously diagonalizable by a common orthogonal matrix  $U$ ). Hence,

$$\text{Tr}(\Sigma_Z^{-1} \text{Cov}(Z|D_\gamma X + Z)(I - D_\gamma^{-2})) = \text{Tr}((I - D_\gamma^{-2})^{1/2} \Sigma_Z^{-1/2} \text{Cov}(Z|D_\gamma X + Z) \Sigma_Z^{-1/2} (I - D_\gamma^{-2})^{1/2}).$$

The argument of the second trace term is clearly positive semidefinite, and therefore (5) holds for all  $\gamma \in [0, 1]$  under the additional assumption that  $A$  and  $\Sigma_Z$  commute, thereby repairing Liu et al.'s proof.

In closing, we remark that the additional assumption that  $A$  and  $\Sigma_Z$  commute is a relatively strong one. It can easily be seen, using the simultaneous diagonalization property of  $A$  and  $\Sigma_Z$  by a common orthogonal matrix  $U$ , that Theorem 1 has a completely equivalent statement where  $Z \sim N(0, I)$  and  $A$  is restricted to be a diagonal matrix with diagonal entries  $0 \leq a_{ii} \leq 1$ ,  $i = 1, \dots, n$ .

## References

- [1] Ruoheng Liu, Tie Liu, H.V. Poor, and S. Shamai. A vector generalization of Costa's entropy-power inequality with applications. *Information Theory, IEEE Transactions on*, 56(4):1865–1879, April 2010.
- [2] M. Costa. A new entropy power inequality. *Information Theory, IEEE Transactions on*, 31(6): pp. 751–760, November 1985.
- [3] Thomas A Courtade. Strengthening the entropy power inequality. In *Information Theory (ISIT), 2016 IEEE International Symposium on*, pages 2294–2298. IEEE, 2016.